MATH 4330 –Final Exam guideline

A. State the followings (30%)

1.

Theorem 5. ***The Division Algorithm*** *If a and b are integers such that $b > 0$, then there exist unique integers q and r such that $a = bq + r$ where $0 \leq r < b$.*

2.

Theorem 22. *1. If a, b, c and m are integers such that $m > 0$, $d = (m, c)$ and $ac \equiv bc(mod\ m)$, then $a \equiv b(mod\ m/d)$.*

2. If $(m, c) = 1$ then $a = b(mod\ m)$ if $ac \equiv bc(mod\ m)$.

3.

Theorem 23. *If*

$$a \equiv b(mod\ m_1), a \equiv b(mod\ m_2), ..., a \equiv b(mod\ m_t)$$

where $a, b, m_1, m_2, ..., m_t$ are integers and $m_1, m_2, ..., m_t$ are positive, then

$$a \equiv b(mod\ \langle m_1, m_2, ...m_t \rangle)$$

4.

Theorem 27. *The system of congruences*

$$\begin{aligned} x &\equiv b_1(mod\ n_1), \\ x &\equiv b_2(mod\ n_2), \\ &. \\ &. \\ &. \\ x &\equiv b_t(mod\ n_t), \end{aligned}$$

has a unique solution modulo $N = n_1 n_2 ... n_t$ if $n_1, n_2, ..., n_t$ are pairwise relatively prime positive integers.

5.

Theorem 28. *Let p be a prime. A positive integer m is its own inverse modulo p if and only if p divides $m + 1$ or p divides $m - 1$.*

6.

Theorem 39. *Let $n = p_1^{a_1} p_2^{a_2} ... p_s^{a_s}$ be the prime factorization of n. Then*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_s}\right).$$

7.

Theorem 58. *If the positive integer m has a primitive root, then it has a total of $\phi(\phi(m))$ incongruent primitive roots.*

8.

Theorem 60. *Consider the prime p and let $p - 1 = kn$ for some integer k. Then $x^n - 1$ has exactly n incongruent roots modulo p.*

9.

Theorem 68. *If $p \neq 2$ is a prime, then there are exactly $(p-1)/2$ quadratic residues modulo p and $(p-1)/2$ quadratic nonresidues modulo p in the set of integers $1, 2..., p-1$.*

10.

Theorem 69. ***Euler's Criterion*** *Let $p \neq 2$ be a prime and let a be a positive integer such that $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\phi(p)/2} (mod\ p).$$

11.

Theorem 71. *Let $p \neq 2$ be a prime. Let a and b be integers such that $p \nmid a$, $p \nmid b$ then*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

12.

Lemma 14. *If $p \neq 2$ is a prime and a is an odd integer such that $p \nmid a$, then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2} [ia/p]}.$$

13.

Theorem 73. ***The Law of Quadratic Reciprocity*** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

B. Proofs (70%)

14.

Show that if n is an odd integer then 8 divides $m^3 - 1$.

15.

Show that if $ac \mid bc$, then $a \mid b$.

16.

If n is an integer, show that $n\,(\,n-1\,)\,(\,2n-1\,)$ is divisible by 6.

17.

If 2 and 3 are not factors of n^2, show that $n^2 + 23$ is divisible by 24.

18.

Show that $3n^2 - 1$ is not a square for any integer n.

19.

Show that if a and b are relatively prime integers, then $(a+2b, 2a+b) = 1$or 3.

20.

Show that if a and b are positive integers where a is even and b is odd, then $(a, b) = (a/2, b)$.

21.

Show that if a, b, m and n are integers such that m and n are positive, $n \mid m$ and $a \equiv b(mod\ m)$, then $a \equiv b(mod\ n)$.

22.

Show that if $\bar{a}$ is the inverse of a modulo m and $\bar{b}$ is the inverse of b modulo m, then $\bar{a}\bar{b}$ is the inverse of ab modulo m.

23.

Let r be a primitive root of p with $p \equiv 1(mod\ 4)$. Show that $-r$ is also a primitive root.

24.

Show that if p is a prime and $p \equiv 1(mod\ 4)$, then there is an integer x such that $x^2 \equiv -1(mod\ p)$.

25. Find all integers that leave a remainder of 1 when divided by 2, a remainder of 2 when divided by 3 and a remainder of 3 when divided by 5.

26. Show that the integer n has a primitive root if and only if the only solutions of the congruence $x^2 \equiv 1(modn)$ are $x \equiv \pm 1(mod\ n)$.

27. Find a congruence describing all primes for which 5 is a quadratic residue.